ISE를 사용하는 vEdge 및 컨트롤러에 대한 RADIUS 및 TACACS 기반 사용자 인증 및 권한 부여

목차

소개

이 문서에서는 ISE(Identity Service Engine)를 사용하는 vEdge 및 컨트롤러에 대한 Radius 및 TACACS 기반 사용자 인증 및 권한 부여를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

데모에서는 ISE 버전 2.6이 사용되었습니다.19.2.1을 실행하는 vEdge-클라우드 및 컨트롤러

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

Viptela 소프트웨어는 세 개의 고정 사용자 그룹 이름을 제공합니다.**basic**, **netadmin** 및 **operator**. 사용자를 하나 이상의 그룹에 할당해야 합니다.기본 TACACS/Radius 사용자는 자동으로 기본 그룹에 배치됩니다.

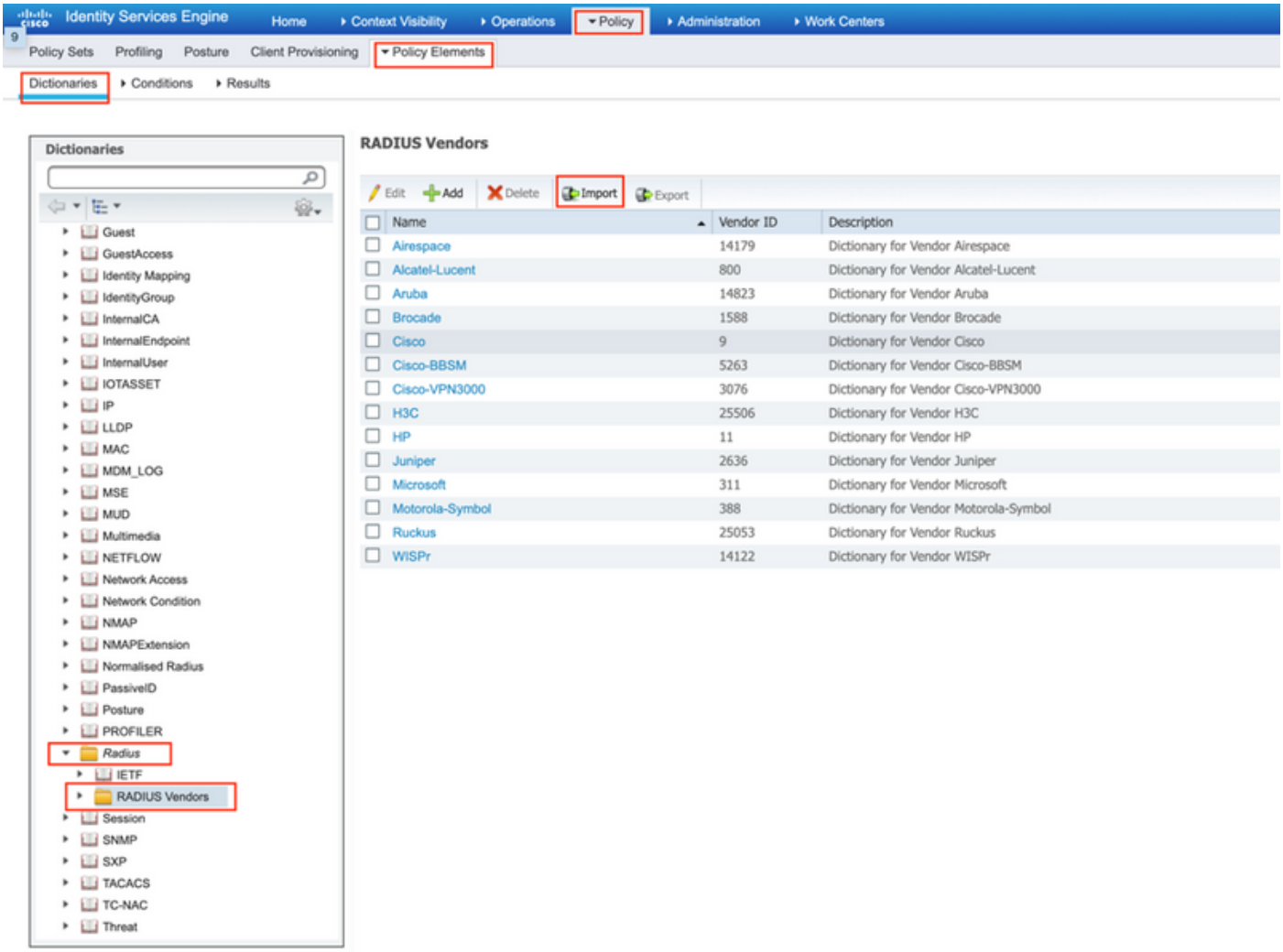
vEdge 및 컨트롤러에 대한 RADIUS 기반 사용자 인증 및 권한 부여

1단계. ISE에 대한 Viptela 반지름 사전을 생성합니다.이렇게 하려면 내용이 포함된 텍스트 파일을

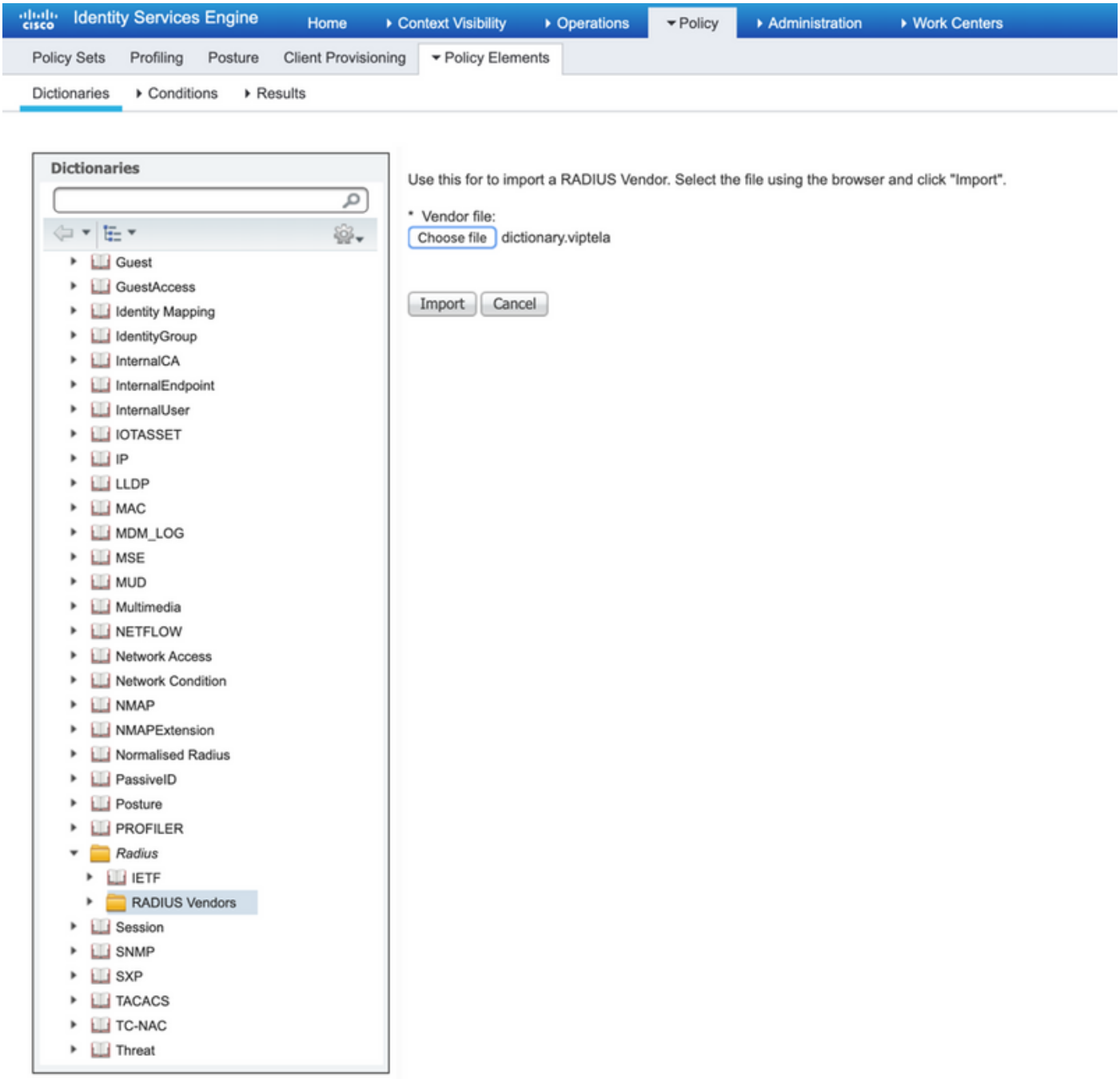
만듭니다.

```
# -*- text -*-
#
#  dictionary.viptela
#
#
# Version:      $Id$
#

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1     string
```

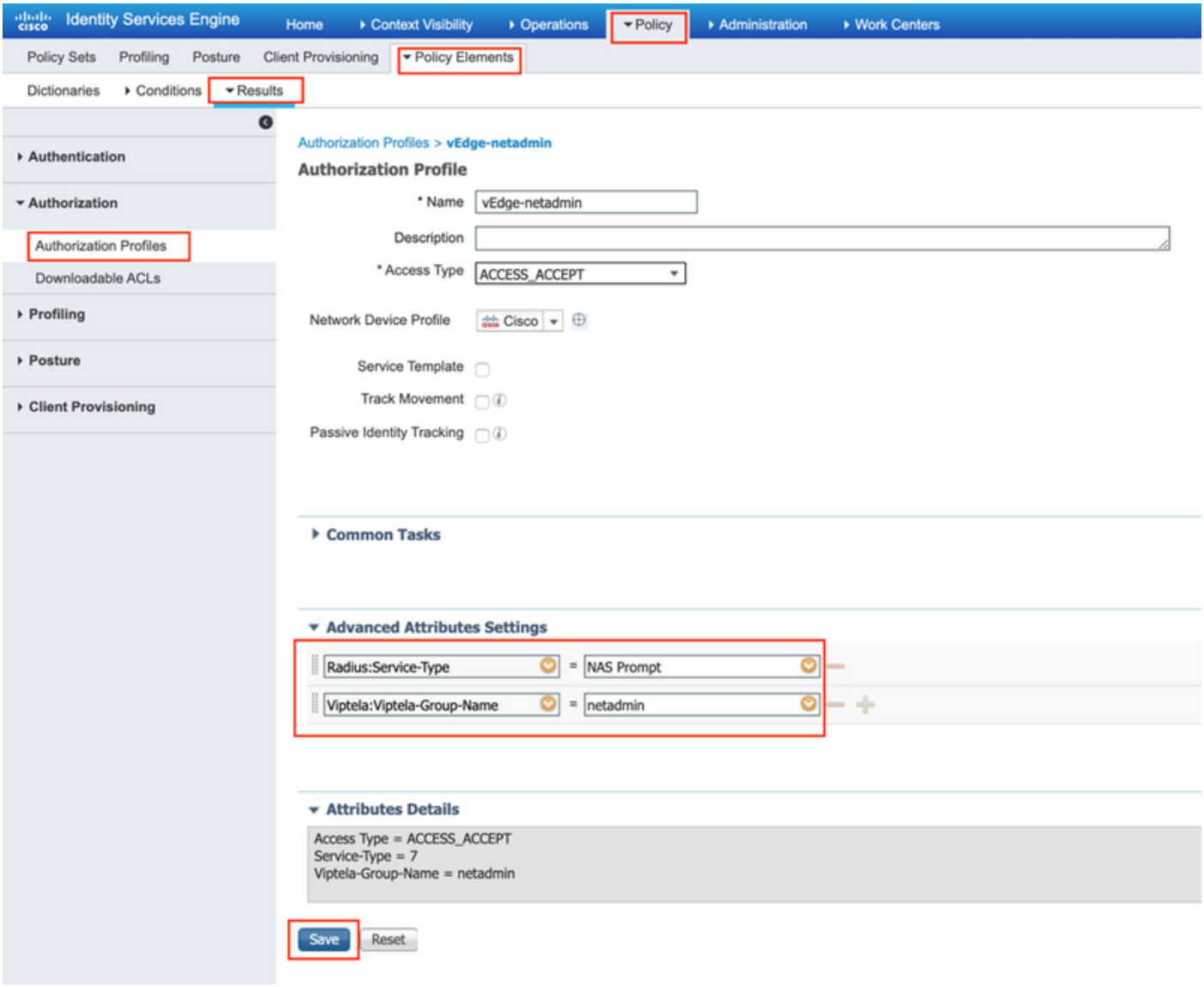
2단계. ISE에 사전을 업로드합니다.이 경우 Policy(정책) **> Policy Elements(정책 요소) > Dictionaries(사전)로 이동합니다**.Dictionaries(사전) 목록에서 Radius(**Radius) > Radius Vendors(RADIUS 벤더)**로 이동한 다음 표시된 이미지와 같이 Import(가져오기)를 클릭합니다.



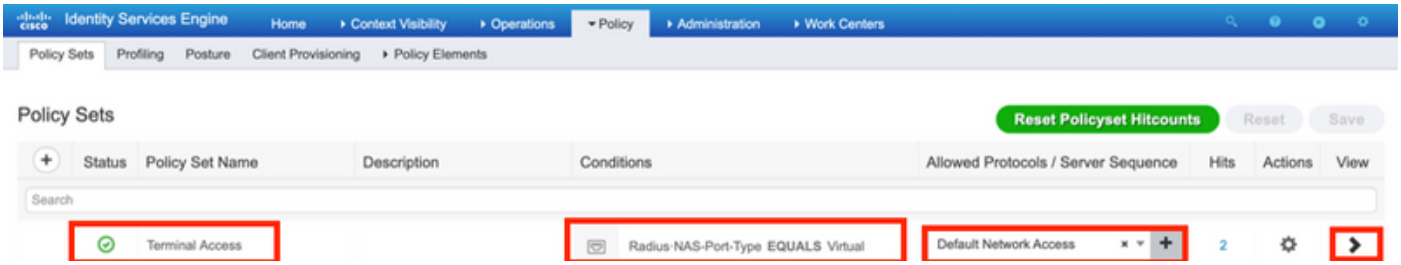
이제 1단계에서 생성한 파일을 업로드합니다.



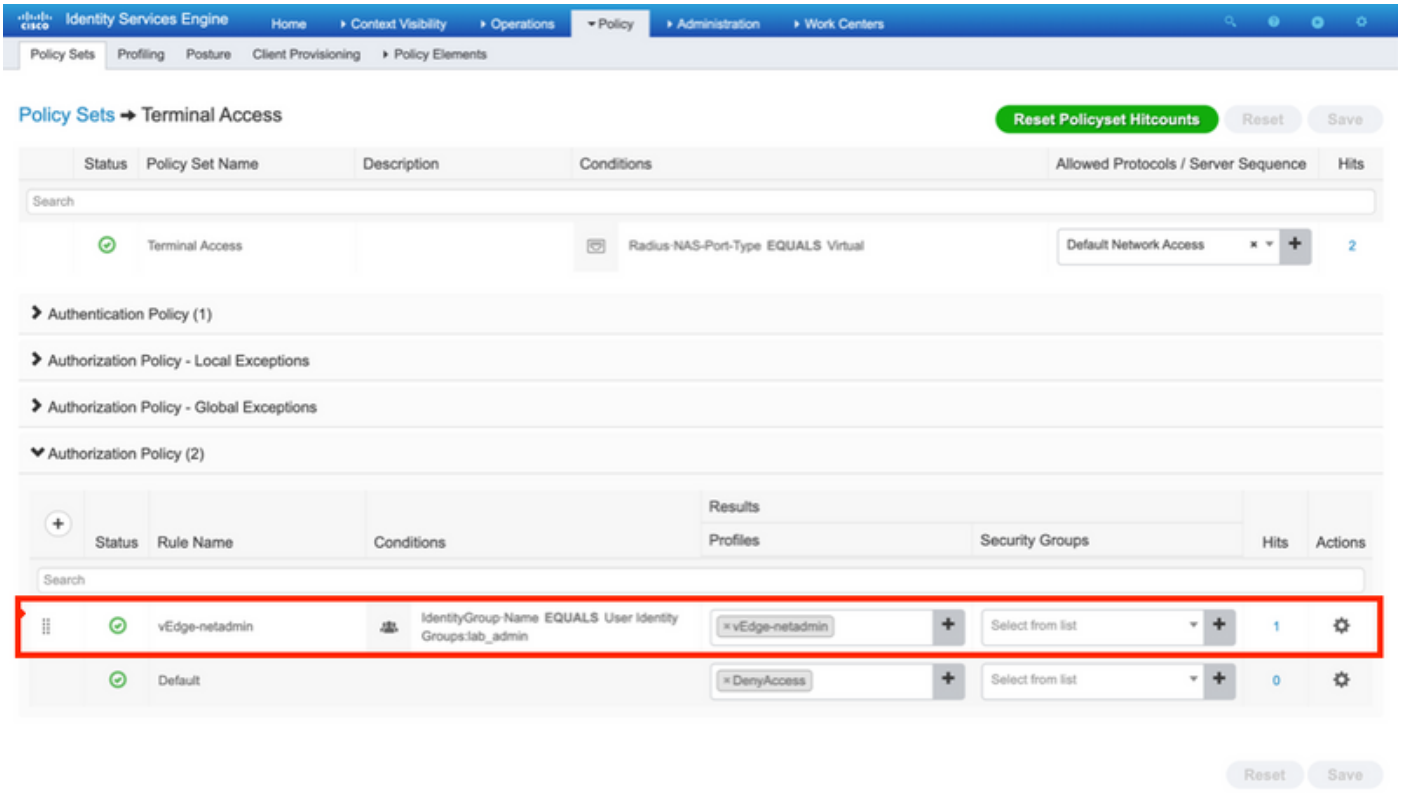
3단계. 권한 부여 프로파일을 생성합니다.이 단계에서 Radius 권한 부여 프로파일은 인증된 사용자에게 다음과 같은 netadmin 권한 레벨을 할당합니다.이를 위해 **Policy(정책) > Policy Elements(정책 요소) > Authorization Profiles(권한 부여 프로파일)로 이동하고** 이미지에 표시된 대로 두 개의 고급 특성을 지정합니다.



4단계. 실제 설정에 따라 정책 세트가 다르게 표시될 수 있습니다.이 문서의 데모에서는 이미지에 표시된 대로 **터미널 액세스라는** 정책 항목이 생성됩니다.

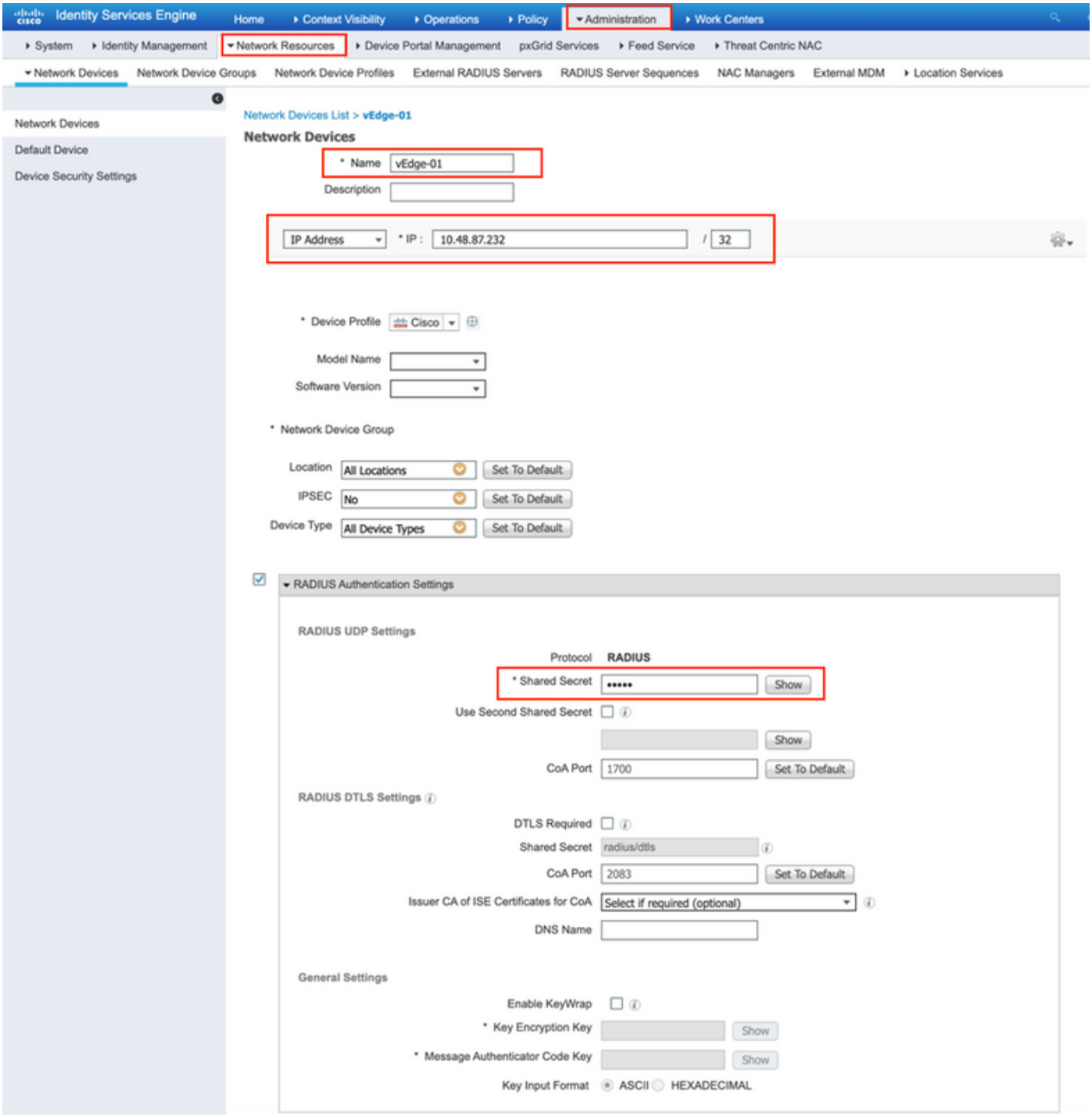


> 을 클릭하면 다음 화면이 이미지에 표시된 것처럼 나타납니다.



이 정책은 사용자 그룹 lab_admin을 기준으로 매칭하며 3단계에서 생성한 권한 부여 프로파일을 할당합니다.

5단계. 이미지에 표시된 대로 NAS(vEdge 라우터 또는 컨트롤러)를 정의합니다.



6단계. vEdge/컨트롤러를 구성합니다.

```
system
 aaa
  auth-order       radius local
  radius
  server 10.48.87.210
   vpn 512
   key cisco
  exit
 !
!
```

7단계. 확인.vEdge에 로그인하여 원격 사용자에게 할당된 netadmin 그룹을 확인합니다.

```
vEdgeCloud1# show users
```

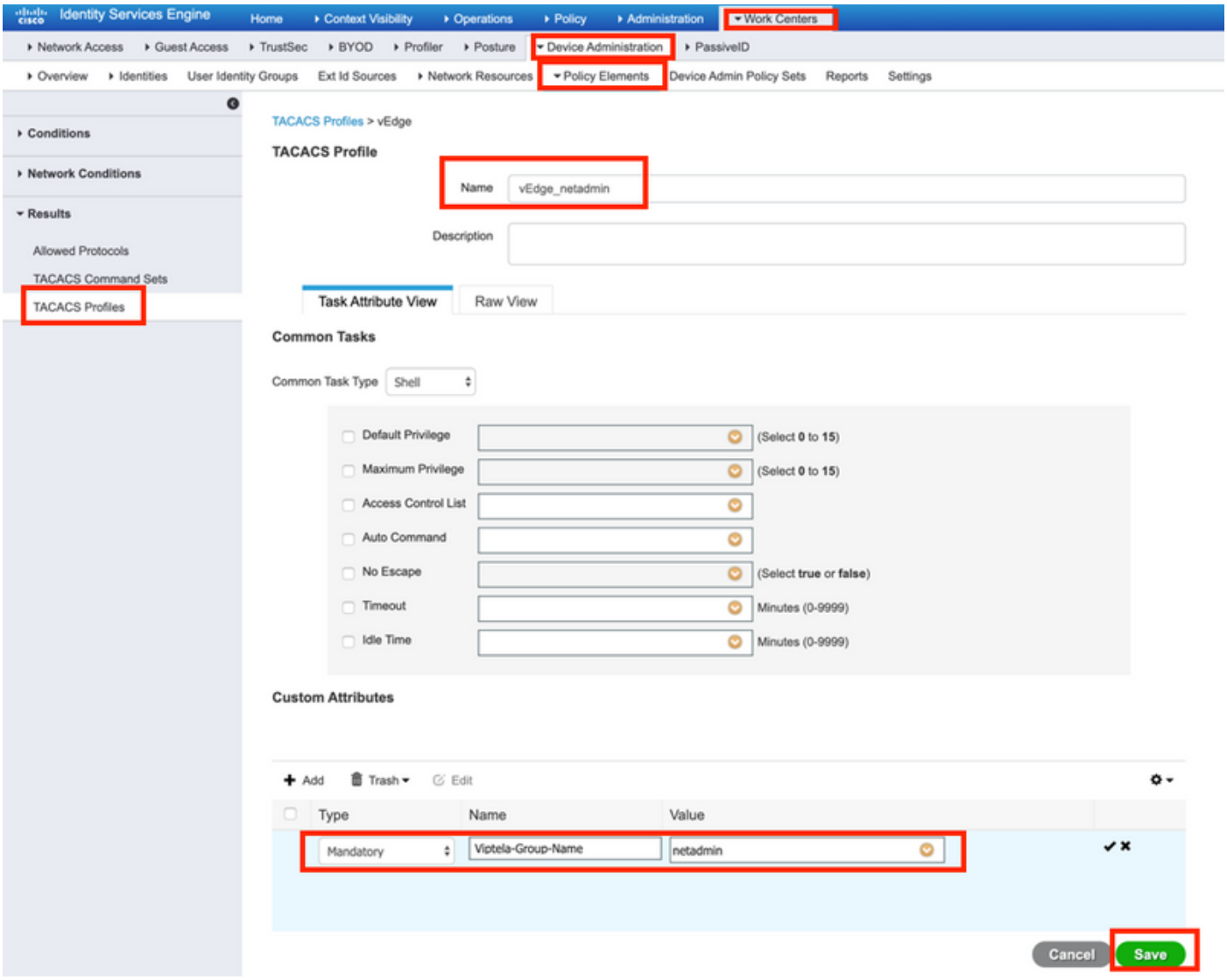
```
                                                    AUTH
SESSION  USER       CONTEXT  FROM           PROTO   GROUP       LOGIN TIME
-------------------------------------------------------------------------------
33472    ekhabaro   cli      10.149.4.155   ssh     netadmin    2020-03-09T18:39:40+00:00
```

vEdge 및 컨트롤러에 대한 TACACS 기반 사용자 인증 및 권한 부여

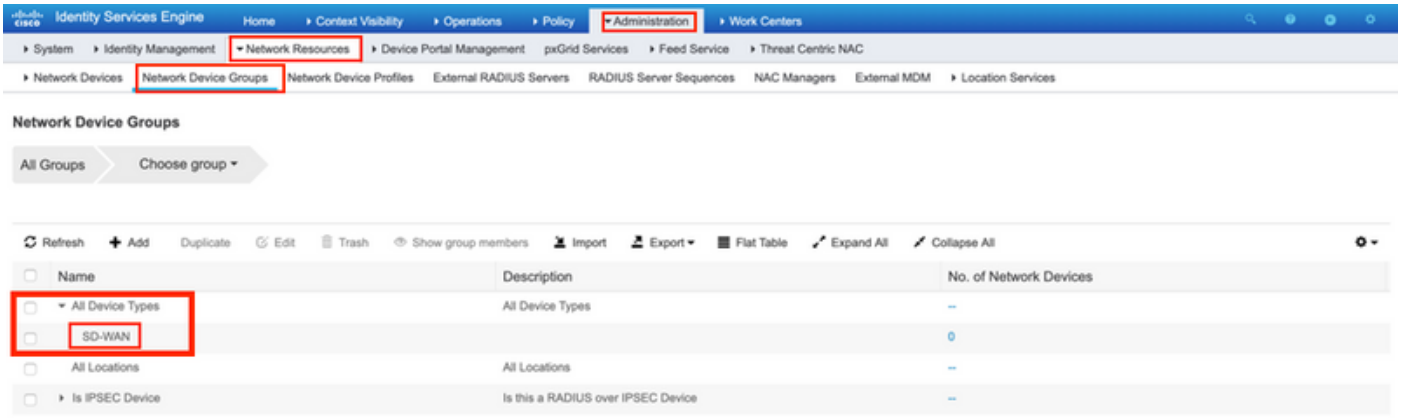
1단계. TACACS 프로파일을 생성합니다.이 단계에서는 생성된 TACACS 프로파일이 할당됩니다(예: netadmin 권한 레벨 인증 사용자).

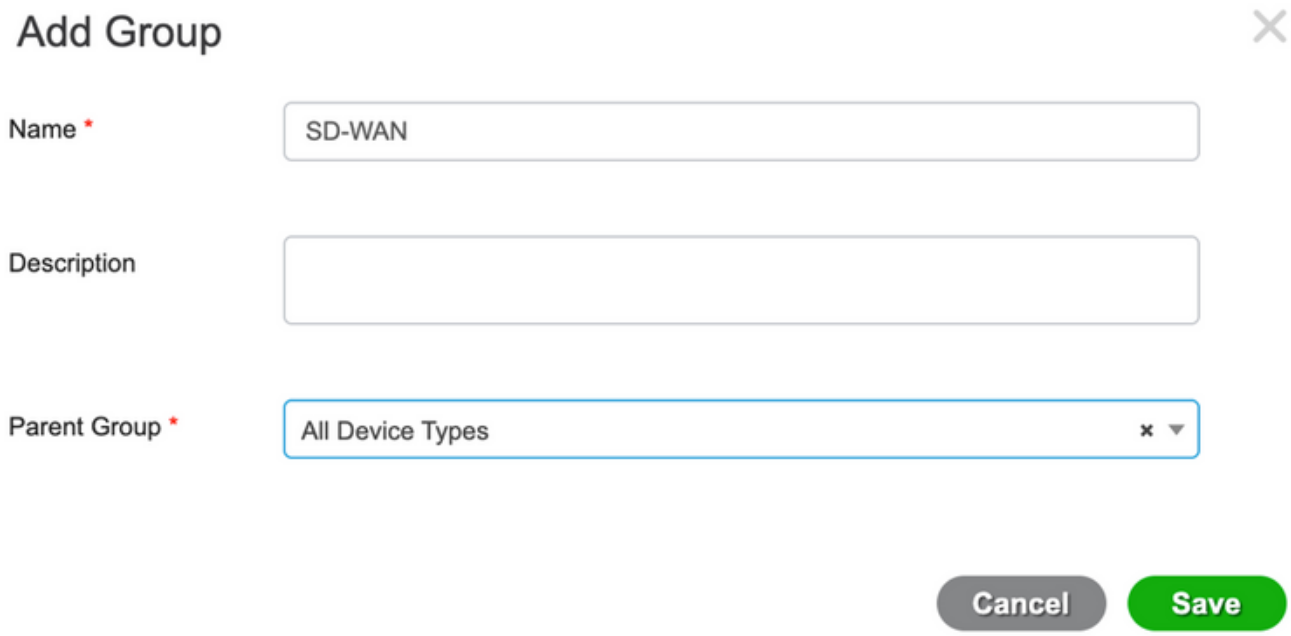
- Custom **attribute(사용자 지정** 특성) 섹션에서 Mandatory(필수)를 선택하여 다음과 같이 특성을 추가합니다.

유형 이름 **가치**
필수 Viptela-Group-Name(비디오-그룹-이름) netadmin

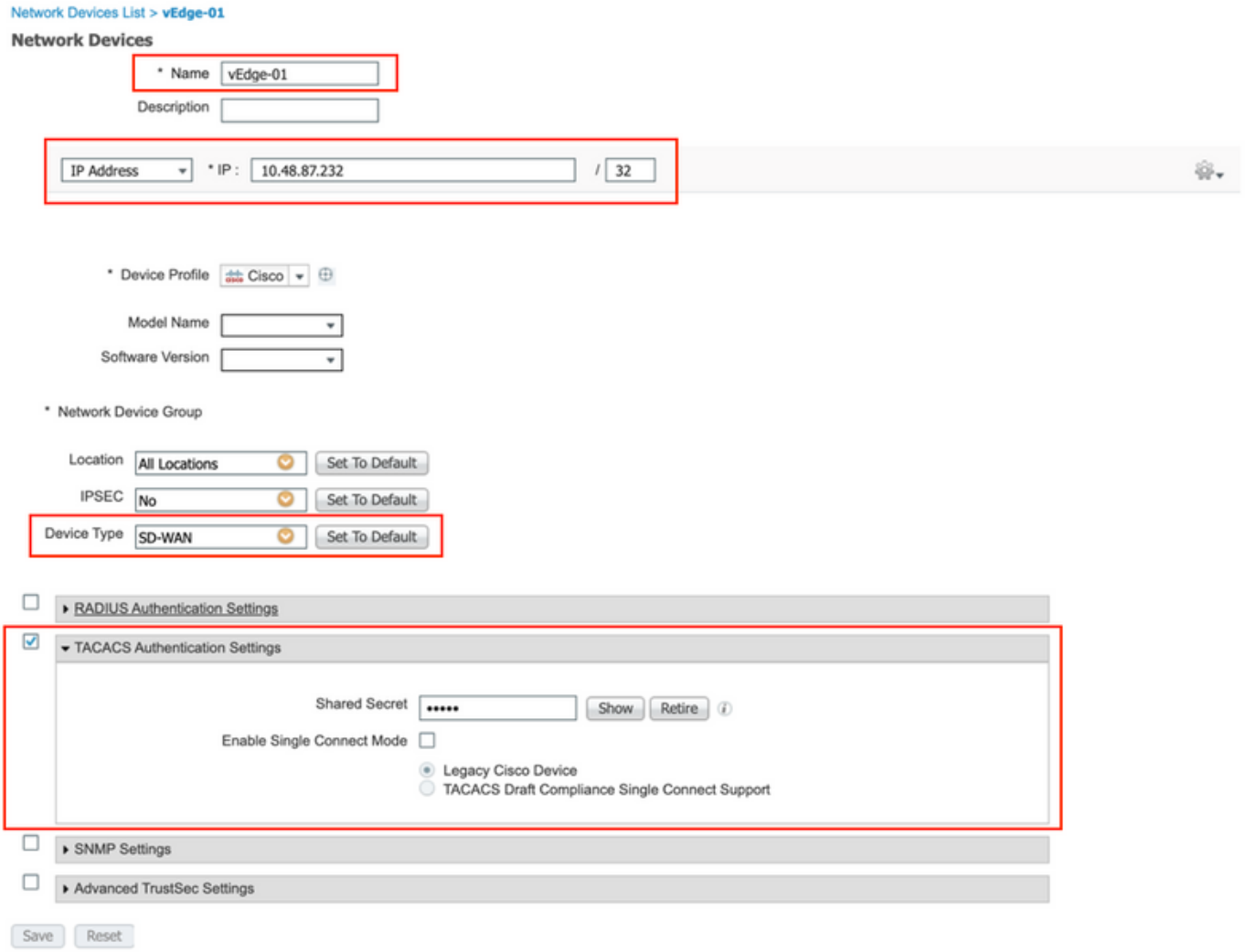


2단계. SD-WAN용 장치 그룹을 만듭니다.



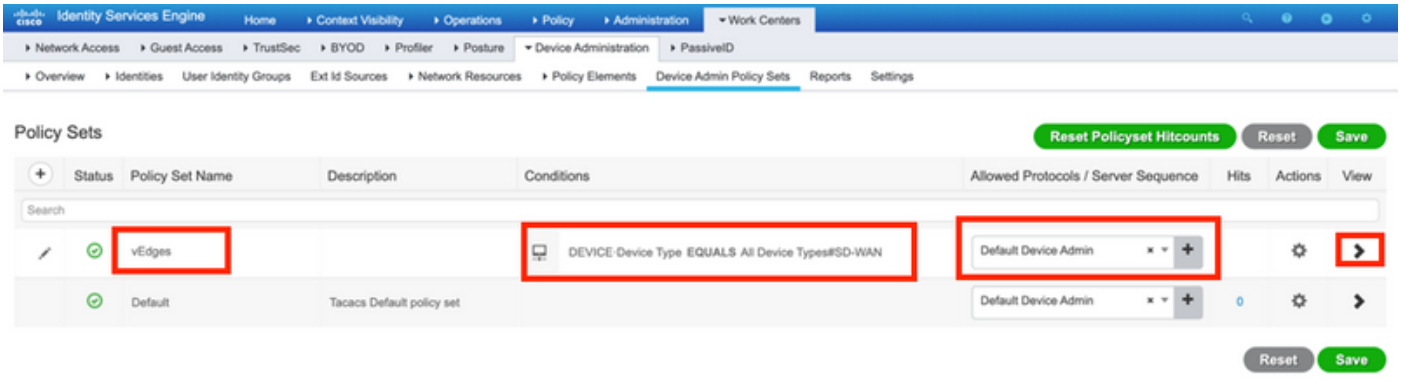


3단계. 디바이스를 구성하고 SD-WAN 디바이스 그룹에 할당합니다.

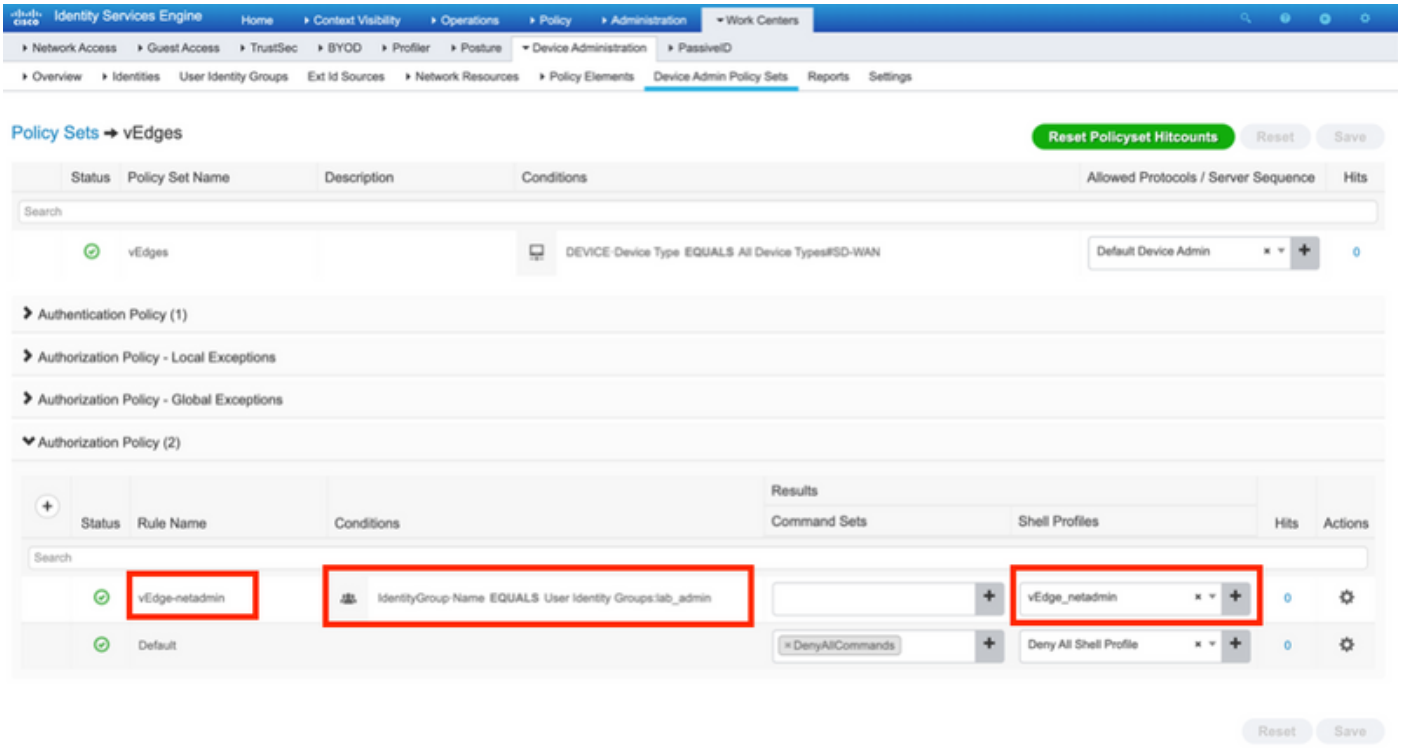


4단계. 디바이스 관리 정책을 정의합니다.

실제 설정에 따라 정책 세트가 다르게 표시될 수 있습니다.이 문서의 데모를 위해 정책이 생성됩니다.



> 을 클릭하면 다음 화면이 이 이미지와 같이 나타납니다.이 정책은 이름이 **SD-WAN**인 디바이스 유형**에** 따라 일치하며 1단계에서 생성된 셸 프로파일을 할당합니다.



5단계. vEdge 구성:

```
system
 aaa
  auth-order tacacs local
 !
 tacacs
  server 10.48.87.210
   vpn 512
   key cisco
  exit
 !
!
```

6단계. 확인.vEdge에 로그인하여 원격 사용자에게 할당된 netadmin 그룹을 확인합니다.

```
vEdgeCloud1# show users

                                                    AUTH
SESSION  USER      CONTEXT  FROM           PROTO   GROUP      LOGIN TIME
-------------------------------------------------------------------------------------
33472    ekhabaro  cli      10.149.4.155   ssh     netadmin   2020-03-09T18:39:40+00:00
```

5단계. vEdge 구성:

5단계. vEdge 구성:

5단계. vEdge 구성:

관련 정보

- Cisco ISE 디바이스 관리 규정 구축 설명서: https://community.cisco.com/t5/security-

documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973

- 사용자 액세스 및 인증 구성: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interfaces/03Configuring_User_Access_and_Authentication